



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,092	10/03/2003	David Andrew Thomas	200309084-1	3543

22879 7590 11/29/2006

HEWLETT PACKARD COMPANY  
P O BOX 272400, 3404 E. HARMONY ROAD  
INTELLECTUAL PROPERTY ADMINISTRATION  
FORT COLLINS, CO 80527-2400

EXAMINER

NGUYEN, KHOI

ART UNIT	PAPER NUMBER
----------	--------------

2196

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

10/679,092

Applicant(s)

THOMAS ET AL.

Examiner

Khoi Nguyen

Art Unit

2196

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-30 are pending in this application and presented for examination.

#### ***Claim Objections***

2. Claims 27 and 29 recites the limitation as below
  - a. "The identifier" of claim 27 in line 7, and "the key" in line 9.
  - b. "the wireless device" of claim 29 in lines 9.

There is insufficient antecedent basis for these limitations in the claims.

#### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
4. Claims 1, 5, 8, 11-12, 15, 20, 27-28, and 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The following phrases are not clearly understood, rendering the corresponding claims vague and indefinite:

- a. "receiving" of claim 1, lines 3, 7, 8; claim 5, line 2; claim 8, line 9; claim 12, line 2; claim 15, lines 3, 4; claim 20, lines 3, 5; claim 27, lines 3, 7, 8; claim 28, lines 2, 6. It is not clearly understood whether the content server, the payment server, or the device is the recipient of the output.
- b. "sending" of claim 1, line 9. It is not clearly understood whether the content server, the payment server, or the device is the sending out information.
- c. "comparing the cyphertext" of claim 15, line 7. It is not clearly understood whether the comparison is done at the content server, the payment server or the device.
- d. "Optionally" of claim 11, line 2. It is not clearly understood which key secret would be used to encrypt the decryption key.
- e. "the identifier" of claim 28, line 2. It is not clearly understood if it is referring to the concealed identifier or any other ordinary identifier.
- f. "the key" of claim 28, line 8. It is not clearly understood if it is referring to the key that is used to encrypt the selected file, the authorization key, or the decryption key.

- g. "the encrypted key" of claim 28, line 9. It is not clearly understood if it is referring to the decryption key or authorization key.
- h. "an encrypted file" of claim 30, line 4. It is not clearly understood if it is referring to the encrypted content file or any ordinary encrypted file.
- i. "an authorization" of claim 30, line 5. It is not clearly understood if it is referring to payment authorization, decryption key authorization, or any ordinary authorization key.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-11, 17, 20-23, 26-30 are rejected under 35 U.S.C 103(a) as being unpatentable over Downs et al. (US Pat. No. 6,226,618), hereafter "Downs", in view of Knox (US. Pub. 2003/0194988), hereafter "Knox".

7. With regard to claim 1, Downs discloses a method for facilitating content downloads via an insecure communications channel (abstract), comprising:

Receiving from a device via an insecure communications channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication) at least one shared secret in encoded form (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret).

transmitting encrypted content (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content) via the insecure communication from a content server to the device (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication.)

receiving a confirmation (Col. 10, lines 57-58, confirmation is inherently drawn from verifying process of the Electronic Digital Content Store(s) or content providers to indicate the request is valid and authentic) authorizing release of a decryption key (Col. 10, lines 19-23, Col. 10, lines -61-63); and

sending the decryption key for decryption of the encrypted content (Col. 10 lines 62-65).

However, Downs does not disclose the shared secret in encoded form that functions as an identifier of the device, and receiving the shared secret in plaintext form via a secure communications channel.

Knox, on the other hand, discloses a shared secret ([0016], lines 6-7, PIN reads on shared secret) form that function as an identifier of the device ([0016], lines 8-9).

In addition, Knox also discloses receiving the shared secret in plaintext form via a secure communication channel ([0016], lines 1-3, conducting registration over the phone reads on secure channel).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox communication between mobile devices and landline devices using fewer number of packet so as to increase transmission efficiency in mobile devices of limited computing resources and to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

8. With regard to claim 2, Downs discloses a method where the confirmation is based on payment for the transmitted encrypted content (Col. 47, lines 42-45).

9. With regard to claim 3, Downs does not disclose the shared secret identifies a user, the device, or both. However, Knox discloses a shared secret ([0016], lines 6-7, PIN reads on shared secret) identifies a user, the device, or both ([0016], lines 8-9).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

10. With regard to claim 4, Down discloses the shared secret (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret), but does not disclose the shared secret is a credit card number or a phone number.

On the other hand, Knox discloses the shared secret ([0016, lines 6-7, PIN reads on shared secret) is a credit card number or a phone number ([0016, lines 8-9].

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to



reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

11. With regard to claim 5, Downs discloses a method of receiving from the device an acknowledgement indicating receipt of the decryption key (Col. 77, lines 44-47, the decryption key is contained within License SC).
12. With regard to claim 6, Downs discloses the decryption key is sent to the device (Col. 10, lines 62-63) via the insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication).
13. With regard to claim 7, Downs discloses sending the decryption key for decryption of the encrypted content via a channel to a point of sale terminal (Fig. 6, End User Device(s) 109, Col. 10, lines 62-63, end user device is read on POS terminal), but does not disclose sending the decryption key for decryption of the encrypted content via the secured channel.

On the other hand, Knox discloses a method of receiving the shared secret in plaintext form ([0016, lines 6-8; account number and PIN associated with the prepaid calling card is considered as a shared secret) via a secure communications channel ([0016], lines 1-3, conducting registration over the phone is read on secure channel).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

14. With regard to claim 8, Downs discloses a method of receiving a random plaintext (Col. 15, lines 63-64, Secure Content or SC contains the random key which reads on random plaintext) from the device (Col. 16, lines 18-19).
15. With regard to claim 9, Downs further discloses the shared secret is encoded (Col. 16, lines 5-6, symmetric key reads on shared secret) by a hash function (Col. 16, lines 7-8) of a combination of the shared secret (Col. 16, lines 9-11, symmetric key digest which contains the encrypted symmetric keys reads on shared secret) and the random plaintext (Col. 15, lines 65-66, content digest reads on random plaintext)
16. With regard to claim 10, Downs further discloses a method of encrypting the decryption key before sending it to the device (Col. 10, lines 61-65).

Art Unit: 2196

17. With regard to claim 11, Downs further discloses decryption key is encrypted (Col. 16, lines 5-6) using at least the shared secret (Col. 16, lines 9-11) and, optionally, the random plaintext secret (Col. 15, lines 65-66).
18. With regard to claim 17, Downs discloses content stored in the content server is encrypted prior to a start of a download process (Fig. 3, Col. 15, step 301, lines 63-64).
19. With regard to claim 20, Downs discloses a method of authorizing a release of a decryption key corresponding to a downloaded content, comprising:  
  
sending a shared secret to a content server (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret).  
  
Receiving a confirmation of successful encrypted content download from the content server (Col. 46, lines 6-7, Content SC contains encrypted content).  
  
Prompting the user to accept terms of download and decryption of the encrypted content (Col. 44, lines 47-49, Store usage conditions read on term of downloading and decryption of content); and

After receipt of an indicia of such acceptance, sending an authorization to the content server to release a decryption key for decrypting the downloaded encrypted content (Col. 10 lines 62-65).

However, Downs does not disclose receiving the shared secret in plaintext form via a secure communications channel.

Knox, on the other hand, discloses a shared secret ([0016, lines 6-7, PIN reads on shared secret) form that function as an identifier of the device ([0016], lines 8-9).

In addition, Knox also discloses receiving the shared secret in plaintext form via a secure communication channel ([0016], lines 1-3, conducting registration over the phone reads on secure channel).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5)

20. With regard to claim 21, Downs discloses a system for transmitting a file to a device, comprising of:

A content server operative to store a plurality of content files (Fig. 1A, component 113, Fig. 6, component 101, Col. 10, lines 3-4, web sites normally store variety of content either locally or remotely which reads on plurality of content files) and transmitting via an insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication).

One or more remote devices operative to transmit and receive communication to and from the content server over the insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication) including any one of the content files in encrypted form (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content), each device including a processor to manage the communications (Col. 81, lines 14-16, web server reads on processor and conducting communication) as well as encryption and decryption of communicated data (Col. 81, lines 62-65).

However, Downs does not disclose transmitting content file wirelessly via an insecure channel.

On the other hand, Knox discloses a prepaid wireless communication system having multiple service providers (Fig. 1 – Component 122 and 124, [0012], lines 1-2).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5)

21. With regard to claim 22, Downs disclose a computer readable program embodied on a computer readable medium for facilitating content download from a content server to a device via an insecure communication channel, comprising:

Program code (Col. 7, lines 37-39, Col. 11, lines 35-36) for causing a computer to receive a shared secret in an encoded form from a device (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret).

Program code (Col. 7, lines 37-39, Col. 11, lines 35-36) for causing a computer to transmit content in an encrypted form (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content) from a content server to the device (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8).

Art Unit: 2196

Program code (Col. 7, lines 37-39, Col. 11, lines 35-36) for causing a computer to receive the shared secret in via a channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on channel).

Program code (Col. 7, lines 37-39, Col. 11, lines 35-36) for causing a computer to receive a confirmation (Col. 10, lines 57-58, confirmation is inherently drawn from verifying process of the Electronic Digital Content Store(s) or content providers to indicate the request is valid and authentic) authorizing the release of a decryption key for the transmitted encrypted file (Col. 10, lines 19-23, Col. 10, lines -61-63); and

Program code (Col. 7, lines 37-39, Col. 11, lines 35-36) for causing a computer to send the decryption key for decrypting the transmitted encrypted file (Col. 10 lines 62-65) for which the payment confirmation has been received (Col. 19, step 138 lines 7-9).

However, Downs does not disclose the shared secret in encoded form that functions as an identifier of the device, and receiving the shared secret in plaintext form via a secure communications channel.

Knox, on the other hand, discloses a shared secret ([0016], lines 6-7, PIN reads on shared secret) form that function as an identifier of the device ([0016], lines 8-9).

In addition, Knox also discloses receiving the shared secret in plaintext form via a secure communication channel ([0016], lines 1-3, conducting registration over the phone reads on secure channel).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

22. With regard to claim 23, Downs discloses computer program embodied on a computer readable medium wherein the confirmation is sent (Col. 19, step 139, lines 14, transaction SC reads on confirmation of purchased goods) upon payment by a user of the device for the downloaded content (Col. 19, step 138 lines 7-9).
23. With regard to claim 26, Downs discloses a computer readable program embodied on a computer readable medium for authorizing a release of a decryption key corresponding to a downloaded content, comprising:



Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for sending a shared secret to a content server (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret).

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for receiving a confirmation of successful encrypted content download from the content server (Col. 46, lines 6-7, Content SC contains encrypted content).

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for prompting the user to purchase the downloaded encrypted content (Col. 19, step 147, lines 30-31); and

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for, after receipt of payment, sending an authorization to the content server to release a decryption key operative to decrypt the downloaded encrypted file (Col. 10 lines 62-65).

However, Downs does not disclose code for receiving the shared secret in plaintext form via a secure communications channel.

Art Unit: 2196

Knox also discloses receiving the shared secret in plaintext form via a secure communication channel ([0016], lines 1-3, conducting registration over the phone reads on secure channel).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5)

24. With regard to claim 27, Downs discloses a method for facilitating content downloads via an insecure communications channel, comprising:

Receiving a concealed identifier (Fig. 6, component 623, Col. 24, lines 9 – 14, encrypted symmetric key reads on concealed identifier).

transmitting encrypted content (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content) via the insecure communication (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication), wherein the encrypted file has a corresponding decryption key (Fig. 1A; Col. 19, lines 30-33, Content SC contains also the corresponding decryption key for each content).

Art Unit: 2196

receiving an authorization from a payment server (Col. 19, lines 7-8) over the insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication)

encrypting the key (Col. 15, lines 63-64, encrypting the symmetric key reads on the key); and

transmitting the encrypted key to the device (Col. 16, Step 307A, lines 18-19)

However, Downs does not disclose the concealed identifier identifies the device; receiving the identifier in an unconcealed form over a secure channel; receive authorization from payment server over the secure channel; and encrypting the key using the identifier.

Knox, on the other hand, discloses a shared secret ([0016, lines 6-7, PIN reads on shared secret) form that function as an identifier of the device ([0016], lines 8-9).

Knox also discloses, receiving the identifier in an unconcealed form [0016], lines 6-8) over a secure channel ([0016], lines 1-3, telephone reads on secure channel).

Art Unit: 2196

Knox also disclose, receive authorization from payment server [0016], lines 3-4, activation at the POS reads on authorization from payment server) over the secure channel ([0016], lines 1-3, telephone reads on secure channel).

Know further discloses using the key as an identifier ([0016], lines 7-8, phone number of the device reads on device identification and simply communicates over a phone line construe the fact that the key does not need to be encrypted).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

25. With regard to claim 28, Downs discloses a method for payment of file downloads to a wireless device, comprising:

Receiving a concealed identifier (Fig. 6, component 623, Col. 24, lines 9 – 14, encrypted symmetric key reads on concealed identifier)

Transferring a selected encrypted file (Col. 19, step 138, lines 7-10) to end-user device (Col. 19, step 139, line 14), wherein the selected file is encrypted using a

Art Unit: 2196

key (Fig. 6 component 641, Col. 19, step 138, lines 7-10, Offer SC contain Content file which encrypted by a symmetric key)

Using an identifier of the algorithm to encrypt the key (Col. 30, lines 45-47); and

Transmitting the encrypted key to the device (Col. 19, step 145 line 34, license SC contains the encrypted symmetric key, which reads on encrypted key) after receipt of payment (Col. 19, step 138 lines 7-10)

However, Downs does not receiving a concealed identifier from a device, wherein the identifier corresponds to the wireless device, receiving the identifier in an unconcealed form over a secure channel as part of payment transaction, using the identifier to encrypt the key, and transmitting the encrypted key to the wireless device

Knox, on the other hand, discloses a shared secret ([0016, lines 6-7, PIN reads on shared secret) form that function as an identifier of the device ([0016], lines 8-9).

Knox also discloses, receiving the identifier in an unconcealed form [0016], lines 6-8) over a secure channel ([0016], lines 1-3, telephone reads on secure

Art Unit: 2196

channel) as part of payment transaction ([0016], lines 3-4, activation at the POS reads on part of payment).

Knox discloses using the key as an identifier ([0016], lines 7-8, phone number of the device reads on device identification and simply communicates over a phone line construe the fact that the key does not need to be encrypted).

Knox further discloses end-user is a wireless device (Fig. 1, [0012] lines 3-5).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

26. With regard to claim 29, Downs discloses a system for transmitting content via an insecure communications channel, comprising:

Means for receiving a shared secret in a concealed form, from a device (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret).

Art Unit: 2196

Means for transferring a selected content in an encrypted form (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content) to the device, wherein the selected file has a corresponding decryption key (Fig. 1A; Col. 19, lines 30-33, Content SC contains also the corresponding decryption key for each content).

Means for receiving encrypted shared secret (Col. 19, step 139 lines 14) over a insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication) as part of a payment transaction (Col. 19, step 138 lines 7-10).

Means for using the shared secret to encrypt a decryption key (Col. 16, lines 9-11).

Means for transmitting the encrypted decryption key to a device (Col. 19, step 145 line 34, license SC contains the encrypted symmetric key, which reads on encrypted key) after receipt of payment (Col. 19, step 138 lines 7-10).

However, Downs does not disclose the shared secret identifies the device, receiving the shared secret in an unconcealed form over a secure channel, and transmitting the encrypted decryption key to the wireless device.

Art Unit: 2196

Knox, on the other hand, discloses a shared secret ([0016], lines 6-7, PIN reads on shared secret) form that function as an identifier of the device ([0016], lines 8-9).

In addition, Knox also discloses receiving the shared secret in plaintext form [0016, lines 8-9, PIN number does not need to be encrypted since it is transmitting over a copper medium (e.g. telephone wire) which deploy certain level of security for the data) via a secure communication channel ([0016], lines 1-3, conducting registration over the phone reads on secure channel).

Knox further discloses end-user is a wireless device (Fig. 1, [0012] lines 3-5).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to reduce additional complication to the customer registration process ([Knox, 0009], lines 4-5).

27. With regard to claim 30, Downs discloses an apparatus for content download to a device via an insecure channel comprising;



Art Unit: 2196

Means for receiving a shared secret in a concealed form from a device (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret).

Means for transmitting an encrypted file to the device (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content).

Means for transmitting after receipt of an authorization (Col. 19, step 138 lines 7-10), a decryption key encrypted using a public key (Col. 19, step 144 lines 30-32, symmetric key, which reads on decryption key is encrypted with end-user's public key which reads on the identifier, wherein can decrypt the encrypted file (Col. 10 lines 62-65).

However, Downs does not disclose means for receiving at least one identifier for a device, where the identifier identifies the device.

Knox, on the other hand, discloses means for receiving identifier of the device ([0016], lines 8-9, phone number of the wireless device reads on identifier of the device).

Art Unit: 2196

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and Knox to the customer registration process ([Knox, 0009], lines 4-5).

28. Claims 12-16 are rejected under 35 U.S.C 103(a) as being unpatentable over Downs, in view of Knox, and further in view of Hirota et al. (US. Pat. No. 6,868,402), hereafter "Hirota"

29. With regard to claim 12 and 14, Downs disclose receiving from the device a content download confirmation value (Col. 77, lines 44-47). However, neither Downs nor Knox discloses the confirmation value is encoded with the shared secret.

On the other hand, Hirota discloses the key/certificate management DB for managing the secret key/public key; the certificates issued from the certificate authorities, and the public keys of the certificate authorities (Col. 13, lines 10-18, private/public keys reads on shared secret).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs, Knox, and teachings of Hirota to establish a submission time stamp defining system capable

Art Unit: 2196

of rationally determining time stamp when a document is submitted via a communication channel (Hirota, Col. 3, lines 2-5).

30. With regard to claim 13, Downs disclose receiving from the device a content download confirmation value (Col. 77, lines 44-47). However, neither Downs nor Knox discloses the shared secret based on an MD5 checksum.

On the other hand, Hirota discloses a document with payment certificate, which will be transmitted, is compressed by using the one-way cryptographic function (Col. 17, lines 13-15, one-way cryptographic function reads on MD5).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs, Knox, and teachings of Hirota to establish a submission time stamp defining system capable of rationally determining time stamp when a document is submitted via a communication channel (Hirota, Col. 3, lines 2-5).

31. With regard to claim 15, Downs discloses the step of receiving confirmation comprises:
- receiving a random plaintext (Col. 15, lines 63-64, Secure Content or SC contains the random key which reads on random plaintext) from the device (Col. 16, lines 18-19)

receiving a hash of the shared secret and the random plaintext for each shared secret (Fig. 4, component 408, 414, and 413, Col. 16, Step 408, line 27, SC contains symmetric-key digest and content digest. Symmetric-key digest contains the symmetric key that reads on shared secret and the content digest reads on random plaintext)

computing a hash of the shared secret with the random plaintext to produce a cyphertext for each shared secret; (Fig. 4, Symmetric-key digest 414 and Content digest, Col. 16, lines 33-35)

comparing the cyphertext to each of the received hash of each of the shared secrets (Fig. 4, Component 414, Col. 16, lines 42-45); and in the case of a match,

identifying the corresponding transmitted encoded content (Col. 16, line 49),

However, neither Downs or Knox discloses encoding a content download confirmation value for the transmitted encoded content using the shared secret; and comparing the computed content download confirmation value to the received content download confirmation value to verify a complete content download

On the other hand, Hirota discloses the key/certificate management DB for managing the secret key/public key; the certificates issued from the certificate authorities, and the public keys of the certificate authorities (Col. 13, lines 10-18, private/public keys are used for encrypt/decrypt content, which reads on shared secret).

Further more, Hirota also discloses the message digest of this overall document data is obtained and is compared with the message digest, which has been stored (Col. 20, lines 13-15, message digest reads on download confirmation value).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs, Knox, and the teachings of Hirota to establish a submission time stamp defining system capable of rationally determining time stamp when a document is submitted via a communication channel (Hirota, Col. 3, lines 2-5)

32. With regard to claim 16, Downs further discloses after verification of the complete content download (Col. 19, step 146, lines 27-29, end-user only receives License SC if pre-verification processes are completed, which allow end-user to

Art Unit: 2196

download content), causing a prompt to be sent to a user of the device to purchase the downloaded content (Col. 19, step 147, lines 30-31), and receiving a confirmation of receipt of payment (Col. 47, lines 42-45).

**33.** Claims 18-19, 24-25 are rejected under 35 U.S.C 103(a) as being unpatentable over Downs, in view of Hirota.

**34.** With regard to claim 18, Downs discloses a method for downloading content from a content server over an insecure communications channel, comprising:

sending a shared secret in an encoded form to a content server (Fig. 6, component 623, Col. 24, lines 9 – 14, symmetric key is the same key needed on both end to encrypt/decrypt content which reads on shared secret) via an insecure communication channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication).

downloading from the content server an encrypted content (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content) via the insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication.)

Art Unit: 2196

receiving a decryption key in an encrypted form from the content server (Col. 10, lines 62-65) via the insecure channel (Fig. 6, Components 101, 103, 105, and 105, Col. 23, lines 4-8, Internet reads on insecure communication), wherein the decryption key is encrypted using the shared secret (Fig. 3, Col. 16, line 5, public key reads on shared secret)

decrypting the downloaded decryption key using the shared secret (Fig. 4., Col. 16, lines 52-53, recipient's private key reads on share secret).

Decrypting the downloaded encrypted content using the decryption key (Col. 16 lines 54-45, symmetric key reads on decryption key); and

Sending an acknowledgement of the received decryption key (Col. 77, lines 44-47, the decryption key is contained within License SC).

However, Downs does not disclose sending an encoded content download confirmation value to the content server via the insecure communication channel.

On the other hand, Hirota discloses the key/certificate management DB for managing the secret key/public key; the certificates issued from the certificate authorities, and the public keys of the certificate authorities (Col. 13, lines 10-18, private/public keys are used for encrypt/decrypt content).

Art Unit: 2196

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and teachings of Hirota to establish a submission time stamp defining system capable of rationally determining time stamp when a document is submitted via a communication channel (Hirota, Col. 3, lines 2-5).

35. With regard to claim 19, Downs discloses an indicia of acceptance of term of the download and decryption of the encrypted content by the user (Col. 44, lines 47-49, Store usage conditions read on term of downloading and decryption of content), where the indicia is an indication of acceptance of payment (Col. 19, step 140 and 141, lines 8-14, End-user requested the download reads on acceptance of payment for selected content).
36. With regard to claim 24, Downs disclose a computer readable program embodied on a computer readable medium for downloading content from a content server, over an insecure communications channel, comprising:  
  
Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for sending a shared secret in an encoded form to a content server (Col. 15, step 301 lines (63-64)).



Art Unit: 2196

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for receiving from the content server an encrypted content (Fig. 1A; Col. 19, lines 30-33, Content SC contains encrypted content).

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for receiving an encrypted decryption key from the content server (Col. 10, lines 62-65), wherein the decryption key is encrypted using the shared secret (Fig. 3, Col. 16, line 5, public key reads on shared secret);

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for decrypting the downloaded decryption key using the shared secret (Fig. 4., Col. 16, lines 52-53, recipient's private key reads on share secret).

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for decrypting the downloaded encrypted content using the decryption key (Col. 16 lines 54-45, symmetric key reads on decryption key); and

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for sending an acknowledgement of the received decryption key (Col. 77, lines 44-47, the decryption key is contained within License SC).

However, Downs does not disclose code for sending an encoded content download confirmation value to the content server via the insecure communication channel.

On the other hand, Hirota discloses the key/certificate management DB for managing the secret key/public key; the certificates issued from the certificate authorities, and the public keys of the certificate authorities (Col. 13, lines 10-18, private/public keys are used for encrypt/decrypt content).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to combine the teachings of Downs and the teachings of Hirota to establish a submission time stamp defining system capable of rationally determining time stamp when a document is submitted via a communication channel (Hirota, Col. 3, lines 2-5)

37. With regard to claim 25, Downs discloses a computer readable program embodied on a computer readable medium further comprising:

Code (Col. 7, lines 37-39, Col. 11, lines 35-36) for providing an indicia of acceptance of term of the download and decryption of the encrypted content by the user (Col. 44, lines 47-49, Store usage conditions read on term of downloading and decryption of content), where the indicia is an indication of

Art Unit: 2196

acceptance of payment (Col. 19, step 140 and 141, lines 8-14, End-user requested the download reads on acceptance of payment for selected content).

### ***Conclusion***

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US Pat. No. 5,850,446 to Berger et al. (Discloses multi-level key encryption of a communication between devices).

b. US Pub No. 2005/0050208 to Chatani (Discloses wireless and land devices communication with high level of e-commerce methods).

c. US Pat. No. 6,148,405 to Liao et al. (Discloses wireless and landnet with plaintext id embedded into session request).

d. US Pat. No 5,629,980 to Stefik et al. (Discloses message transmission, session initiation, and authorization transactions in general).

e. US Pub. No. 2004/0198220 to Whelan et al. (Disclose wireless device communication in roaming environment).


Art Unit: 2196

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on M-Fri (7:30-5:00) Fri (7:30 - 4:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil E. El Hady can be reached on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KN  
Khoi Nguyen

  
NABIL M. EL-HADY  
SUPERVISORY PATENT EXAMINER